State of Illinois

Department of Central Management Services

SECURITY POLICY

Effective January 30, 2007

Public Distribution
Version 1.0

SECURITY POLICY

Effective January 30, 2007

Version 1.0

APPROVAL SHEET

EXPEDITED APPROVAL

BCCS Deputy Director: _____ Date: _____

If approved digitally (via email), attach copy & write subject line & date below.

Owner: _____ Date: _____

If approved digitally (via email), attach copy & write subject line & date below.

Policy Review Board Chair: _____ Date: _____

If approved digitally (via email), attach copy & write subject line & date below.

Return to Policy Review Board Chair

Expedited publications MUST be formally submitted to the Policy Review Board within 180 days from the BCCS Deputy Director approval date in order to undergo customary review and stakeholder comment or the publication will be withdrawn and retired.

TABLE OF CONTENTS

POLICY STATEMENT

State resources must be protected from unauthorized access, use, disclosure, alteration, modification, deletion, destruction, damage, or removal.

PURPOSE

The purpose of this policy is to outline actions and authorize procedures that ensure state resources are adequately protected and secure.

BUSINESS CASE

State and federal law as well as best business practice require that an organization's assets be secure and protected and that the integrity and confidentiality of data be maintained. Inadequate protection of physical and/or logical resources can result in financial loss as well as loss of customer confidence and could result in litigation proceedings against the organization or specific individuals within the organization.

RELEVANCE

Communications Act

Computer Crime Prevention Law

Computer Fraud and Abuse Act

Computer Security Act

Disposal Act (Data Security on State Computers

Economic Espionage Act

Electronic Commerce Act

Electronic Communications Privacy Act

Federal Information Security Management Act

Federal Privacy Act

Gramm-Leach-Bliley Act

Health Insurance Portability & Accountability Act (HIPAA)

National Information Infrastructure Protection Act

Patriot Act

Whistleblower Protection Act (state & federal)

SCOPE

This policy applies to any state IT resource (as defined in Definitions) for which the Illinois Department of Central Management Services manages, maintains, operates, stores, or is otherwise held accountable.

This policy does not address human safety. Other policies, procedures, and plans address the top priority of human health and safety. These include but may not be limited to emergency (or incident) response plans, evacuation plans, personal conduct rules, emergency management plans, public health procedures, and homeland security guidelines and recommendations.

This policy, and the resulting set of procedures, address ISO 17799[1] criteria. ISO 17799 criteria states that a security policy and resulting procedures should cover the following areas: system access control, computer & operations management, system development and maintenance, physical and environmental security, compliance, personnel security, security organization, asset classification and control, and business continuity.

DEFINITIONS

The following terms are used in this policy. For additional information on a specific term, click on the term below to display its definition or find it in the Shared Services Glossary.

- *Appropriate Business Unit*
- *Authorized / Unauthorized*
- *Security Screening / Background Check*
- *Classification*
- *Confidential*
- *Custodian/Owner*
- *Data/Information*
- *Due Diligence*
- *Inappropriate*
- *IT Resource*
- *ISO 17799*
- *Logical*
- *Physical*
- *Revoke*
- *IT State Resource*
- *User*
- *Whistleblower*

ENFORCEMENT

Noncompliance with this policy and/or its resulting procedures may be cause for disciplinary action up to and including discharge, may involve civil or criminal litigation, and may involve financial assessment, restitution, fines, or penalties.

[1] ISO 17799 is an internationally recognized standard consisting of a comprehensive set of controls representing best practices in information security. More information is available at www.iso-17799.com

RESPONSIBILITY

Each user of a state resource is responsible for following the intent of this policy, any published procedure(s), and due diligence.

Anyone observing what appears to be a breach of security, violation of this or other state policy, violation of state or federal law, theft, damage, or any action placing state resources at risk must report the incident to an appropriate level supervisor, manager, or security officer within their organization. Those reporting alleged incidents will be protected from retaliation by existing whistleblower protection laws currently enforce.

Resource custodians are responsible for ensuring that appropriate and adequate protection and controls are applied to each resource under their care.

Managers and supervisors are responsible for ensuring that workers follow the intent of this policy and are adhering to all related procedures.

Each business unit is responsible for publishing procedures and operational manuals that detail specific actions that implement this policy.

Designated business units, as identified by the Director and/or designee in subsequent operational procedures, are responsible for monitoring and tracking compliance to this policy.

To the extent that is operationally feasible and cost-effective, standards of responsibility will be followed as set forth in ISO 17799 and an appropriate defense-in-depth strategy.

No action or authority defined in this policy will be used to harass, belittle, intimate, or otherwise violate a worker's right to a safe, secure, nurturing environment.

POLICY

- Preventative, detective, and corrective controls must be established, enforced, and monitored to ensure that state resources are protected from unauthorized access, use, disclosure, alteration, modification, deletion, destruction, damage, or removal.

- Appropriate business units will establish, institute, and publish procedures to enhance the protection of state resources. The Bureau of Communications and Computer Services shall establish an organizational unit devoted to resource security with oversight authority over all other business units related to the responsibility of securing and protecting state resources.

- A security screening review (background check) may be conducted on any individual requesting access to any state resource (physical or logical). Access may be delayed until the review is completed. Access may be denied based on impartial analysis of facts uncovered by the review.

- A data classification hierarchy shall be established to assist in delineating proper protection procedures. Different levels of protection will be assigned to the different levels of data classification. Classification will be assigned based on the degree of negative impact (business risk), data value, level of personally identifiable information, and legal or ethical ramifications in the event of unauthorized access, use, and/or disclosure.

- No expectation of privacy exists when a state resource is accessed or used. That is, authorized personnel may review, monitor, track, audit, or otherwise view any resource and/or activity including but not limited to e-mail, Internet, private disk drives, office furniture, etc.

- Appropriate designated personnel are assigned the responsibility and authority to access, audit, review, monitor, trace, intercept, recover, block, revoke, restrict, delete, or disclose (within policy and procedural limitations) any action, data, or behavior involving a state resource.

- All knowledge and information which may be derived or acquired from access to state resources or from access to state premises, respecting secret, confidential, or proprietary matters of the State, shall for all time and for all purposes be regarded as strictly confidential and be held in trust and solely for State of Illinois benefit and use and shall not be directly or indirectly disclosed to any person other than authorized personnel without appropriate written permission.

- Awareness programs and practices will be established to ensure users are knowledgeable in how to use and protect IT resources (including but not limited to hardware and information).

- Incident response plans will be developed detailing steps to be taken in the event security is breached or other negative event occurs.

- Only when deemed necessary by the resource custodian or other appropriate organizational unit (Inspector General, Director's Office, security, etc.) will log monitoring occur and be maintained to assist in intrusion detection, unauthorized access identification, or other protective reasons. Logs must be marked FOIA (5 ILCS 140/) ***exempt*** - based on Section 7, (1)(b), (c), (p), (ii).

REVISION HISTORY

Created: May 1, 2006
Revised: Nov 17, 2006 / Sep 6, 2006 / June 26, 2006 / 12/18/2006
Reviewed: Nov 17, 2006
Effective: Jan 30, 2007

- End of Security Policy -